



UNCLASSIFIED



North Dakota Homeland Security Anti-Terrorism Summary



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including Schools
and Universities\)](#)

[International](#)

[Information Technology and
Telecommunications](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials
Sector](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Commercial Facilities](#)

[Public Health](#)

[Communications Sector](#)

[Transportation](#)

[Critical Manufacturing](#)

[Water and Dams](#)

[Defense Industrial Base Sector](#)

[North Dakota Homeland Security
Contacts](#)

[Emergency Services](#)

NORTH DAKOTA

Texas firm temporarily plugs leaking ND oil well. A ruptured oil well in western North Dakota was temporarily plugged on September 3 after leaking more than 2,400 barrels of crude and water, company officials said. A spokesman for Denbury Onshore LLC of Plano, Texas said the company had done a successful static kill by pumping heavy mud in the well that began leaking early September 1 about 2.5 miles southwest of Killdeer, North Dakota. Crews began pumping the mud into the well immediately after the spill was detected, and it stopped leaking at about 1 a.m. on September 3, he said. Source: <http://www.miamiherald.com/2010/09/03/1806874/texas-firm-temporarily-plugs-leaking.html>

REGIONAL

(Minnesota) Man, 69, accused of mailing white powder, obscene note. A 69-year-old Twin Cities, Minnesota, man has been charged in connection with mailing a suspicious white powder along with an obscene note to Dow Jones & Co. in response to a magazine offer he received from the company. The man, of Long Lake, Minnesota, was charged in an indictment unsealed September 8 in federal court in Minneapolis with false information and hoaxes for allegedly sending the note and the powder, which turned out to be baking flour. According to the indictment: On May 10, the man mailed an obscene note and white powder to a Dow Jones mail facility in Massachusetts. The mailing was in response to a magazine offer he had received from the company. His return note requested, among other things, that he be removed from the company's mailing list. When a mail facility employee opened the note and discovered the powder, a portion of the facility was evacuated. A local hazardous-materials team was summoned to determine whether the powder posed a biological threat. Source: <http://www.startribune.com/local/102472294.html?elr=KArks:DCiUHc3E7 V nDaycUiD3aPc: Yyc:aU U>

(Montana) Man arrested after Missoula hazmat scare. Police in Montana arrested a 24-year-old man after a three-hour long hazardous materials ordeal with a suspicious package in the Missoula Police Department parking lot. Hazmat technicians determined the package to be an iced tea container with some sort of liquid in it, but that the liquid, iced tea or not, was not a threat. The Missoula Police Department says the man who dropped the box later arrived on scene to confess, and was taken to a hospital for an evaluation, but he will be cited. The package was found around 5 p.m. September 6, and the regional hazmat team, as well as the Missoula city and Missoula County bomb squad were immediately assembled. The suspicious package was laced with threatening messages written on the box. While Missoula police would not comment on what exactly was written, one person on scene Monday night said the words "radioactive" were written on the box which naturally escalated the threat level. Source: <http://www.kxih.com/news/man-arrested-after-missoula-hazmat-scare/>

UNCLASSIFIED

(South Dakota) Bomb threat evacuates SD offices building. A bomb threat at the South Dakota State Offices building shuts down business for several hours and forces the evacuation of more than 200 employees. The call came in to police just before 8 a.m. September 7 morning. Police say the South Dakota Offices building became the target of a bomb threat, after an employee found a letter inside the mailbox. "There was reason to believe something may happen in the building at a certain time, so we took precautions to make sure everybody was safe," said a Sioux Falls police lieutenant. At least a dozen officers responded to the call, blocking off every entrance. But the Department of Labor administrator says it was the safety procedure already in place, that provided the most security for everyone inside. According to officials, there were several customers inside doing business when the letter surfaced, but they were allowed to leave. Employees were taken across the street, to the Labor Tempel. After searching the entire building, police did not find anything suspicious inside but say evacuating the building was the right thing to do. After more than 3 hours, nearly 200 employees were let back in. Source:

http://www.kdlt.com/index.php?option=com_content&task=view&id=4914&Itemid=57

NATIONAL

(Pennsylvania) Pa. Homeland Security document talks of possible 'environmental extremists'. An intelligence bulletin from the Pennsylvania Office of Homeland Security is circulating on the Internet, and it quotes the FBI as saying that "environmental extremists" are likely to become an increasing threat to energy companies. The governor's press secretary confirmed to Channel 4 Action News on September 9 that the document is real. "Five acts of vandalism over the last two weeks," he said. "Two of those involved firearms — firing of shotguns that put holes in equipment at Marcellus Shale drilling sites" in Venango County. The director of the Marcellus Shale Coalition released the following statement on September 9: "...as the issue of responsible Marcellus development has evolved from a technical consideration to a political one, we've started to see an uptick in the volume and intensity of activism — some of which appears to be directed at preventing our industry from safely delivering these resources to Pennsylvanians. From our point of view, as long as those activities remain generally civil and within the confines of a spirited public debate, there's absolutely no reason for concern. But to the extent they go in the other direction, and potentially devolve in a manner that undermines our ability to keep our folks safe, then we will have a problem." Source:

<http://www.thepittsburghchannel.com/r/24945359/detail.html>

(Michigan) 15,000 without power due to high winds; 1 arson suspect arrested. About 15,000 DTE Energy customers were without power after wicked winds on September 7 ripped down power lines across Wayne County and sparked numerous fires in Detroit. At one point on Tuesday, the winds knocked out service to as many as 50,000 customers, the utility said. A cold front moved in to the region, bringing winds of up to 49 mph, according to the National Weather Service reporting station in White Lake Township. At least two dozen homes caught fire in four hours Tuesday, taxing the ability of firefighters to keep up with the blazes. The winds were blamed with knocking down power lines that caused fires and then quickly spreading the fires to adjacent buildings, Detroit Fire officials said. Arson also was being looked at as a cause for some of the fires. Officers with the Detroit Police Northeastern District arrested a man Tuesday on allegations he possessed a stolen car and further investigation has led officials to believe the man is a suspect for setting fires on Robinwood near Van Dyke, police said. Source: <http://www.detnews.com/article/20100908/METRO/9080398/1410/15-000-without-power-due-to-high-winds--1-arson-suspect-arrested>

UNCLASSIFIED

INTERNATIONAL

Denmark raises terror preparedness after hotel blast. Denmark raised its terror attack preparedness September 11 after a man set off a small explosion in a Copenhagen hotel September 10. After the explosion, police surrounded the suspect in Orsted Park and security personnel removed a bag wrapped around his waist with remote controlled cutting pliers. The man has injuries to his face and arm from the blast, police said. No one else was hurt. A police spokesman said Friday the bag probably did not contain explosives as it had not exploded when shot at. The suspect, who remains in hospital, was not cooperating with police. He said the suspect appeared to be European or North African and around 40 years old and spoke excellent English. Police found a gun at the Hotel Jorgensen in central Copenhagen where the blast occurred in a toilet. Daily newspaper Ekstrabladet, citing police sources, said police had found a map with the address of daily Jyllands-Posten's headquarters in the city of Arhus circled among the man's belongings. Jyllands-Posten's publication in 2005 of cartoons of the Prophet Mohammad provoked protests in the Middle East, Africa and Asia in which at least 50 people died. A Copenhagen court ruled Saturday the man would be detained in custody until October 4 on suspicion of aiming to put others' lives at risk, a police spokesman said. Source: <http://www.reuters.com/article/idUSTRE68A1AE20100911>

Explosives found at power plant in Caucasus. Staff at a hydro-electric power station in Russia's volatile North Caucasus found explosives in what appears to have been a bid to blow up the plant, Russian news agencies reported September 9. Staff found the makeshift explosive device following a fire at the Irganaiskaya power plant in Dagestan the night of September 7, the RIA Novosti agency reported, quoting law enforcement officials. It had been planted underneath the main hydroelectric unit, the agency said. "It was equipped with an electric detonator," the news agency quoted a law enforcement source as saying. "Apparently, they planned to remotely detonate the explosive device." Experts from the country's FSB security service neutralized the device, news agencies reported. The regional branch of the emergencies ministry had earlier reported that the fire at the plant was caused by a technical failure, indicating there were no signs of foul play. But the Interfax news agency, citing an unidentified local law enforcement official, said that one of the plant's employees had gone missing just before the fire broke out and authorities were now looking for him. Source: http://www.khaleejtimes.com/DisplayArticle08.asp?xfile=data/international/2010/September/international_September424.xml§ion=international

Mexican drug cartels cripple Pemex operations in basin. The network of pipes, wells, and tankers belonging to the gigantic Mexican state oil company Pemex have long been an easy target of crooks and drug traffickers who siphon off natural gas, gasoline, and crude, robbing the Mexican treasury of hundreds of millions of dollars annually. Now the cartels have taken sabotage to a new level: They have hobbled key operations in parts of the Burgos Basin, home to Mexico's biggest natural gas fields. In May, gunmen kidnapped five Pemex workers as they rode to the front gate of the Gigante No. 1 natural gas plant in the Burgos Basin. They have not been heard from since. Also reported is the disappearance of at least 30 other employees of subcontractors in the same region. A confidential report submitted to the U.S. Congress in July and made available to the Los Angeles Times acknowledged that stolen natural gas and delayed gas production have cost the company nearly \$50 million in the first 5 months of 2010. One of the U.S. firms working in Burgos, Halliburton, has spoken of a deteriorating security situation slowing its work. But Halliburton said it had no plans to pull any

of its 600 workers. Kidnappings represent just one twist in broad security problems haunting Pemex. Engineers detect hundreds of clandestine siphons every year that steal enormous quantities of petroleum, much of which is then smuggled to the United States and sold at market price. Source: <http://articles.latimes.com/2010/sep/06/world/la-fg-mexico-pemex-20100906>

First suspects charged under Jamaica's new cyber law. Two men in Jamaica have become the first individuals in the country to be arrested and charged under the new Cyber Crimes Act, which was passed last December. The men were charged last week following an investigation that started August 28, Jamaica Observer reports. Earlier that day, the accused men were seen acting suspiciously in a car in front of an ATM in Manchester, which is located in the west-central part of the island. When police searched the men and the vehicle, they found electronic devices used to intercept transactions and to duplicate the PIN and other personal information of customers using the ATM. The men were charged under sections 3, 6 and 8 of the Cyber Crimes Act, and are to appear in court August 8. Source: <http://www.thenewnewinternet.com/2010/09/07/first-suspects-charged-under-jamaicas-new-cyber-law/>

BANKING AND FINANCE INDUSTRY

A cybercriminal's shopping list. According to cybercrime market data scheduled to be published by EMC's RSA Security unit on September 13, the cost of behaving badly online is becoming more affordable than ever. For example, fraudsters can obtain credit card (CVV2) data for around \$1.50 to \$3. Social Security numbers and dates of birth can be obtained for about the same price. "Full" data sets — including the consumer's online banking credentials (e.g., username and password), mailing address, card number, CVV2 code, card's expiration date, data of birth, and SSN — go for \$5 to \$20. Online banking accounts can be purchased for \$50 to \$1,000 per account, depending on the account type and balance. A distributed denial of service (DDoS) attack service costs about \$50 for each 24 hours when launched at a single target. "Bulletproof" hosting services — the hosting of malicious content on law enforcement-resistant platforms — can be leased for as little as \$87 to \$179 a month. A Zeus Trojan kit goes for \$3,000 to \$4,000. "Various fraud products and services are sold in the underground for not more than \$50, but can be associated with the loss of thousands of dollars in the end," RSA says in its report. Source: <http://www.darkreading.com/authentication/security/privacy/showArticle.jhtml?articleID=227400186&subSection=Privacy>

(Virginia) Stolen funds from University of Virginia recovered. The nearly \$1 million that was stolen from a satellite campus of The University of Virginia in late August has been recovered, according to the school's student newspaper. KrebsOnSecurity.com reported September 2 how thieves stole the funds after hacking the computer of the university's comptroller. The attackers used a virus to steal the online-banking credentials for the university's accounts at BB&T Bank, and initiated a fraudulent wire transfer in the amount of \$996,000 to the Agricultural Bank of China. The student newspaper The Highland Cavalier reported September 3 that the vice chancellor for finance and administration had alerted faculty and staff in an e-mail on August 27 that a hacking incident had occurred on campus. He said that no personal data had been compromised. The college's director of news and media relations said the stolen funds have since been recovered. "No funds have been lost," she told The Highland Cavalier. "We caught it early on." Source:

UNCLASSIFIED

<http://www.thenewnewinternet.com/2010/09/07/stolen-funds-from-university-of-virginia-recovered/>

New vishing spree strikes U.S. In July, two phone-based phishing, or vishing attacks, hit residents in Provo, Utah. In August, 10 additional attacks were reported, incorporating a combination of vishing and text-message-based smishing scams, aimed at various communities scattered throughout the United States. The common factor: Perpetrators targeting customers of community banking institutions. "Recently, we've seen them pop up in low-fraud, small places," hitting markets where consumers might not be so savvy or prepared for a socially engineered attack, says the individual who oversees client relations for FICO's Card Alert Service, which provides decision management and predictive analytics solutions for card issuers. Vishing and smishing have replaced the traditional e-mail phishing attacks that were more prevalent three years ago, he says. Since January, the documented number of traditional e-mail or phishing attacks has significantly dropped. "What's replacing them are these new waves of text and person-to-person scams," he says, "and they're not being tracked." August's vishing and smishing schemes hit residents in Elgin, Illinois.; Long Island, New York; Binghamton, New York; New York's Chautauqua and Cattaraugus counties; Bend, Oregon; Arkansas City, Arkansas; Rocky Mount and Henry County, Virginia; Auburn, Alabama; Texarkana, Texas; and Central Falls, Rhode Island. Rather than being generic, in most cases, the calls and texts identified specific institutions by name. Source:

http://www.bankinfosecurity.com/articles.php?art_id=2896

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

(Illinois) Blast hits uranium plant in Illinois 'home' to Superman. A small explosion at a uranium conversion plant in Metropolis, Illinois, has added fuel to the fire of an ongoing labor dispute. The incident occurred September 5 at the Honeywell Metropolis Works. It was just one day after company-hired replacement workers restarted production of the nation's sole uranium conversion plant after a two-month shutdown. No one was injured. No damage was done to the facility. And no dangerous materials were involved, according to the company and regulators. The lockout was the subject of a Post-Dispatch article in early August, detailing how the Ohio River town, which bills itself as Superman's hometown, was nervous about replacement workers handling dangerous materials after the June 28 lockout of 220 union workers. The union called the event "an explosion" and said replacement workers "blew up" part of the plant. Honeywell said it was "a noise" and not unexpected. In a statement, Honeywell called the union's characterization of what happened as "irresponsible and wrong." A spokesman for the NRC which had inspectors on the scene at the time of the incident, confirmed that a small explosion happened during the venting of hydrogen gas.

Source: http://www.stltoday.com/business/article_28f3dbf1-20fa-5ead-a970-fe54459f6440.html

COMMERCIAL FACILITIES

(Connecticut) GOP Senate hopeful at Conn. event with bomb threat. A bomb threat forced the evacuation of a political fundraiser in Connecticut attended by a Republican U.S. Senate candidate. The candidate was among more than 60 people at the home of the Madison Republican Town Committee Chairman September 12. Police say someone called them shortly after 4:30 p.m. to report a bomb at the home. State police searched the house for about an hour and determined the threat

UNCLASSIFIED

was bogus. Source:

<http://www.google.com/hostednews/ap/article/ALeqM5h1EAP5wJXGP0YibJS4G32aSE2qsQD9I709EO0>

(Alabama) U.S. attorney's office looks at charges for explosive device found at WalMart. The police department in Montgomery, Alabama, said it has identified two men in connection with a case involving a live ordnance found in the parking lot of a local WalMart. Now, the U.S. District Attorney's office is looking into possible charges over the incident. The men left the unexploded ordnance in the parking lot of the Ann Street WalMart around noon September 4. Units responded to the scene of a possible grenade and located a live 40 mm round that had been placed in the front parking lot closest to the store. The Montgomery Police Department's Bomb Squad responded, took charge of the devices, and rendered it safe. Authorities acquired video evidence of the suspects and released their images to the media. One suspect turned himself in after seeing the story on TV. He said the incident was all a poor decision by himself and the other person, and that they were just trying to get rid of the device. Police said they are still searching for the second suspect, and though he is not identified to the media, they do know who he is. Source: <http://www.wsfa.com/Global/story.asp?S=13121867>

DOJ investigating at least 5 anti-Muslim acts. The Department of Justice is investigating a handful of apparently anti-Muslim incidents in Texas, Tennessee, California, and New York. FBI agents and civil rights division investigators also are looking into vandalism and other incidents at mosques or mosque construction sites. The open criminal investigations were confirmed by civil rights division spokeswoman in response to a query from the Associated Press. The incidents have followed sustained criticism of the planned mosque near the former site of the World Trade Center in lower Manhattan in New York City. Early plans for the project, known as Park51, call for a 500-seat auditorium, a September 11 memorial, and prayer space. Among the incidents under investigation as potential hate crimes, all dating from July and August: A Muslim cab driver in New York City had his face and throat slashed in a suspected hate crime. Arson was committed at the site of a future mosque in Murfreesboro, Tennessee, where leaders of the local Islamic Center won permission in the spring to build a new mosque after outgrowing their rented space. A brick nearly smashed a window at the Madera Islamic Center in central California, where signs were left behind that read, "Wake up America, the enemy is here," and "No temple for the god of terrorism." A fire was set and graffiti was left at the Dar El-Eman Islamic Center in Arlington, Texas. Police arrested five teenagers after the son of one of the founders of a mosque in Waterport, New York, on Lake Ontario was sideswiped by a sport utility vehicle. One teen was charged with firing a shotgun in the air near the mosque a few days earlier. Source:

<http://www.google.com/hostednews/ap/article/ALeqM5hy6JrOX5CbcySP025oWWyRZ7YPfAD9I3BSC80>

(Alabama) Police: 81-year-old dies in explosion he set off. An 81-year old man died in an explosion he set off intentionally in his third-floor room at a senior citizens home in Decatur, Alabama, police said September 7. The man was killed about 9:30 p.m. September 6 at Summer Manor Apartments, a complex managed by the Decatur Housing Authority. "It was determined the explosion was the result of the intentional detonation of a homemade incendiary device," a Decatur police sgt. said. The housing authority evacuated 75 residents to a nearby motel, and one with a medical condition was taken to a hospital as a precaution, officials said. Source:

UNCLASSIFIED

<http://www.montgomeryadvertiser.com/article/20100908/NEWS02/9080370/Police++81-year-old+dies+in+explosion+he+set+off>

(Alabama) Roller derby dispute led Mobile woman to set off pipe bomb at rink, try to burn house, feds say. A Mobile, Alabama, woman whose roommate was kicked off a women's roller derby team sought vengeance by setting off a pipe bomb at the skating rink and trying to set fire to a team member's home, federal investigators testified last week. According to testimony and an affidavit filed by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the woman admitted to setting off a pipe bomb at the Dreamland Skate Center August 21. The blast damaged a 10-ton air conditioning unit but did not cause injuries. The affidavit alleges that the 32-year-old Mobile woman also admitted to making two other bombs — a Molotov cocktail that she set off at the rink July 7, and a pipe bomb that she threw into the driveway of a Mobile Roller Derby team member with the defendant's roommate. The woman told authorities that she did not know about the bomb, but ATF agents searched the area and found an explosive device in a neighbor's yard, according to court records. Source: http://blog.al.com/live/2010/09/federal_court_digest_mobile_wo.html

(Nevada) Las Vegas casino evacuated after bomb threat. A man claiming to have a bomb around his chest prompted an evacuation of a Las Vegas casino for several hours September 5. The Las Vegas Review-Journal and Las Vegas Sun report that the threat turned out to be a hoax and the man was arrested after the incident at Arizona Charlie's Hotel and Casino. Police say the man apparently wanted to commit "suicide by cop." Police say the man walked up to the security desk inside the casino and showed a security guard what he said was an explosive device. Guards persuaded him to go outside and evacuated the resort. The incident also prompted the temporary closure of the Boulder Highway outside the casino. Source: http://www.google.com/hostednews/ap/article/ALeqM5iBwCZstEwJ1XckxGSpV3xVLjB8_wD9I1E67G0

(Oklahoma) Wildfire in northwestern Oklahoma leads to evacuation of 500. A power line downed by high winds is being blamed for a wildfire that caused the evacuation of 27 homes and 110 camp sites August 6 near Guthrie, Oklahoma. Fire crews from several municipalities battled a grass fire fanned by high winds that burned a 30-acre area. The fire was contained quickly, he said, but fire crews remained on site to put out hot spots two hours after the first responders arrived. The fire started when a power pole snapped because of 40 mph winds. About 500 people were evacuated, and one abandoned mobile home was destroyed. Firefighters from Woodward, Fort Supply, Buffalo, Fargo, Gage and Tatesby fought the blaze. Source: <http://newsok.com/broken-power-pole-is-cited-in-wildfire/article/3492501>

COMMUNICATIONS SECTOR

(New Jersey) Three charged with cutting telephone lines in Salem, other counties for scrap; damage estimated at \$1M. Three Pittsgrove, New Jersey residents have been charged with theft in connection with the cutting of telephone wire from utility poles near Pittsgrove Township, state police said September 8. The value of the stolen wire, and the cost of materials and labor to restore thousands of Verizon customers' service, is estimated by the telecommunications company at \$1 million, state police said. A 30-, 35- and 44-year-old were arrested in connection with the incidents, according to state police. They were charged with theft, criminal intent, conspiracy to commit theft,

UNCLASSIFIED

UNCLASSIFIED

and criminal mischief, police said. The materials were reportedly sold on the scrap metal market. According to reports, police said a Verizon employee contacted the Bridgeton Barracks of the state police September 3 after observing multiple sections of telephone wire that had been cut on Almond Road, and were left on the shoulder of the roadway. After responding to the area, troopers reportedly located one suspect leaving a corn field near Parvins Mill Road and Garden Road, according to state police. Police said they learned the three individuals were allegedly responsible for stealing telephone cable in Salem, Gloucester and Cumberland counties. Source: http://www.nj.com/salem/index.ssf/2010/09/three_charged_with_cutting_tel.html

New method predicts communication-disrupting solar activity. Major solar eruptions (coronal mass ejections) normally take several days to reach the Earth, but the largest recorded in 1859 took just 18 hours. Solar flares — which can also cause significant disruption to communications systems — take just a few minutes. So advance warning is of vital importance to enable steps to be taken to avoid the worst effects of solar activity. Up to now, solar weather prediction has been done manually, with experts looking at 2D satellite images of the sun and assessing the likelihood of future activity. The team from Bradford University's Center for Visual Computing, though, has created the first online automated prediction system, using 3D images generated from the joint NASA/ESA Solar and Heliospheric Observatory satellite (SOHO). Already in use by both NASA and the European Space Agency (ESA), the Bradford Automated Solar Activity Prediction system (ASAP) identifies and classifies sun spots and then feeds this information through a model that can predict the likelihood of solar flares. The system is able accurately to predict a solar flare six hours in advance and the team is working to achieve a similar accuracy for the prediction of major solar eruptions in the near future. The ASAP model is based on historical data, which was analyzed to identify patterns in the sun's activity. Qahwaji is now applying for more funding to further improve the system and ensure it can be adapted to work with the latest sun-monitoring satellites. Source: <http://homelandsecuritynewswire.com/new-method-predicts-communication-disrupting-solar-activity>

IPv6 transition poses new security threats. The countdown to the saturation of the IPv4 address supply is now down to a matter of months, and along with the vast address space of the next-generation IPv6 architecture comes more built-in network security as well as some new potential security threats. IPv6 has been in the works for over a decade now, but with the exhaustion of the IPv4 address space expected anywhere from spring to June of 2011, the long transition to the new IP may finally be on the radar screen for some organizations. Unlike its predecessor, the "new" protocol was built with security in mind: it comes with IPSec encryption, for instance, and its massive address space could help prevent worms from propagating, security experts say. But its adoption also poses new security issues, everything from distributed denial-of-service attacks to new vulnerabilities in IPv6 to misconfigurations that expose security holes. Source: http://www.darkreading.com/vulnerability_management/security/perimeter/showArticle.jhtml?articleID=227300083&subSection=Perimeter+Security

FCC to finalize rules. The U.S. Federal Communications Commission says it plans to finalize rules for the use of wireless Internet devices on unused TV airwaves, an initiative that has been touted by Google Inc., Microsoft Corp. and other technology companies. The FCC said that usage of so-called white-spaces spectrum is on its agenda for the commission's next open meeting September 23. While the use of white-spaces spectrum was approved by the FCC in 2008, the initiative has since bogged

UNCLASSIFIED

UNCLASSIFIED

down as proponents and critics argued over the best way to use vacated airwaves without interfering with other signals. Use of the vacated white spaces became possible thanks to the transition to digital TV transmissions. Google has made a concerted effort to lobby for the use of the white spaces, which could provide stronger wireless-Internet access than what's currently available through Wi-Fi connections. Source: <http://www.omaha.com/article/20100907/MONEY/709079969>

CRITICAL MANUFACTURING

Kia recalls 56,000 Souls, Sorentos in U.S., S. Korea. Kia Motors said September 3 it had started a recall of some 56,000 Soul and Sorento vehicles sold in the United States and South Korea due to defective wiring harnesses that could cause fires. Some harnesses supplied by Johnson Controls for lighting in 2010 model-year Soul cars and 2011 model-year Sorento SUVs were improperly soldered, leading to possible electrical shorts, Kia said in a letter to U.S. safety regulators on August 30. There were no reports of accidents or injuries due to the issue, which was identified in June 2010. The U.S. recall covers 23,972 Soul cars produced from September 7, 2009, through June 8, 2010, and 11,213 Sorento vehicles built from October 23, 2009, through July 30, 2010, according to the notice filed with the U.S. National Highway Traffic Safety Administration. Source: <http://www.reuters.com/article/idUSTRE68202720100903>

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

Study discourages immediate evacuation after nuclear strike. In the initial aftermath of a nuclear strike on a major urban area, airborne radiation would place evacuees in greater danger than individuals who remain deep inside buildings or underground areas, Stanford University analysts concluded in a study published in late August. Congestion along possible evacuation routes would force people attempting to flee the site of a nuclear attack to withstand long periods of exposure to radiation, unless they learn of an impending strike well in advance, United Press International quoted a Society for Risk Analysis statement as saying. "The logistical challenge of an evacuation appears to be beyond current response capabilities," said a Stanford management science professor who is one of the authors of the study. Past research has indicated that emergency workers would probably need 12 to 48 hours after a nuclear strike to set up exit sites. Source: http://www.globalsecuritynewswire.org/gsn/nw_20100908_2660.php

9 years after 9/11, Public Safety Network still a dream. Despite \$7 billion in federal grants and other spending over the last seven years to improve the ability of public safety departments to talk to one another, most experts in such communications say that it will be years, if ever, before a single nationwide public safety radio system becomes a reality. In the meantime, public safety and homeland security officials have patched together voice networks in some regions, including New York, that link commanders at various agencies. But the focus in Washington has turned to the development of the next generation of emergency communications, wireless broadband, which seeks to succeed where radio has failed. "For a brief moment in time, a solution is readily within reach," the

UNCLASSIFIED

UNCLASSIFIED

chief of the Federal Communications Commission's public safety and homeland security bureau told a Congressional hearing this summer. "Unless we embark on a comprehensive plan now, including public funding, America will not be able to afford a nationwide, interoperable public safety network."

Source: http://www.nytimes.com/2010/09/07/business/07rescue.html?_r=1&src=busln

(California) Protest over fatal shooting by LAPD turns violent. A protest over the fatal police shooting of a Guatemalan immigrant turned violent when some demonstrators threw bottles at officers, set trash cans on fire and refused to disperse. The protest began in the afternoon with demonstrators marching back and forth between a bustling shopping area where the shooting occurred and the Rampart police station three blocks away. Television news footage showed people tossing the bottles and plastic crates at officers in riot gear late September 6 near MacArthur Park, a neighborhood with a large Central American population west of downtown Los Angeles, California. Police declared the protest an unlawful assembly around 10 p.m. and ordered the dozens of protesters to disperse. The majority of the crowd cleared out, but a small number lingered and caused trouble. Police arrested and booked four people on suspicion of inciting a riot. Three officers were bruised but did not require hospitalization and went back on duty, and the confrontation was over by about 2 a.m.

Source: http://www.google.com/hostednews/ap/article/ALeqM5gREzQQDTEsm9naE3aIZkpn_orNyAD9I34HL80

ENERGY

(Georgia) 3 men arrested outside Effingham power plant. The Effingham County Sheriffs Department has arrested three men who were found hanging outside a power plant. The three men, two of whom are originally from Russia and the other from Kazakhstan, were found with bolt cutters, a shovel, rubber gloves, and face masks, along with other hand tools. Sheriffs deputies located the men outside the Georgia Power Plant McIntosh in Springfield over the weekend of September 3. Effingham County called in the Joint Terrorism Task Force to further investigate the situation. The men were charged with Possession of Tools during the Commission of a Crime. Source:

<http://www2.wsav.com/news/2010/sep/09/3-men-arrested-outside-effingham-power-plant-ar-809473/>

NIST guidelines tackle the security issues that accompany smart grid. A final set of guidelines for a smart-grid security architecture has been released by the National Institute of Standards and Technology, outlining how security requirements will be incorporated into the design of the nation's next-generation power distribution system. "The United States has embarked on a major transformation of its electric power infrastructure," the interagency report states. "This vast infrastructure upgrade — extending from homes and businesses to fossil-fuel-powered generating plants and wind farms, affecting nearly everyone and everything in between — is central to national efforts to increase energy efficiency, reliability, and security; to transition to renewable sources of energy; to reduce greenhouse gas emissions; and to build a sustainable economy that ensures future prosperity." But security challenges will come with the new intelligent infrastructure. "While integrating information technologies is essential to building the smart grid and realizing its benefits, the same networked technologies add complexity and also introduce new interdependencies and vulnerabilities," the report states. "Approaches to secure these technologies and to protect privacy

UNCLASSIFIED

must be designed and implemented early in the transition to the smart grid.” Source:

<http://gcn.com/articles/2010/09/03/nist-smart-grid-security-guidelines.aspx>

FOOD AND AGRICULTURE

(Michigan) Seven more horses stricken with EEE. With seven more horses dead in Michigan the week of September 6 from Eastern equine encephalitis, health officials are repeating the advice they have given since the disease outbreak began in July: People should avoid being bitten by mosquitoes and horse owners should get their animals vaccinated. The most recent cases include two horses in Calhoun County and one each in Allegan, Kalamazoo, Jackson, Eaton and Shiawassee counties. That brings the summer’s total for cases diagnosed by laboratory testing or clinical observation of symptoms to 119. Laboratory testing has confirmed that 42 Michigan horses have been stricken by the disease; one 3-year-old gelding in Barry County survived, but the rest died. An additional 77 have been diagnosed as having had the deadly mosquito-borne virus based on their symptoms. Only four of those horses are still alive. The affected counties, according to Michigan Department of Agriculture records, are: Allegan, Barry, Branch, Calhoun, Cass, Eaton, Hillsdale, Jackson, Kalamazoo, Livingston, Oakland, St. Joseph and Shiawassee. Six horses have died without a county of residence recorded.

Source:

http://www.mlive.com/news/kalamazoo/index.ssf/2010/09/seven_more_horses_stricken_wit.html

(New York) Menands dairy plant recalls some milk products. A dairy from Menands, New York is voluntarily recalling a variety of milk products sold throughout the North Country under four different brand names. The recalled milk products are all sold in plastic containers and packaged under the brand names Midland Farms, Corrado’s Market, Jersey Dairy Farms and Trade Fair Premium. All of the recalled products — which were sold in New York, Connecticut, Massachusetts, New Jersey and Rhode Island — bear the plant code “36-1661.” Some of the recalled products include gallons of milk, 2 percent milk, 1 percent milk and fat-free milk from Midland Farms, Corrado’s Market and Trade Fair Premium with date code “SEP24.” New York’s state agriculture commissioner alerted consumers September 8 that the recall was due to a potential improper pasteurization. The problem was detected by New York State Department of Agriculture and Markets milk inspectors during an equipment inspection September 7, when they found a failure of pasteurization equipment at the plant. While the recalled products have not been found to be contaminated with any harmful pathogens, the company is recalling the products as a precautionary measure. Source:

<http://pressrepublican.com/breaking2/x885939614/Menands-dairy-plant-recalls-some-milk-products>

(Colorado) Bug sails into Colorado, destroys potatoes. A potato blight has hit northern Colorado. The crop yield is low while the potatoes themselves are small and rough. Small bugs called psyllids are to blame. They landed in Colorado in large numbers this year after high winds from Texas and Mexico gave them a lift. “We just had the right weather patterns in June,” an insect specialist at Colorado State University said. The bugs latch onto the leaves of the potato plants and damage them with their saliva. “This insect damages plants in ways no other insect damages plants,” she said. “It’s the effects of its saliva, which has toxic and systemic effects on the plant that’s really remarkable.” The man who runs Strohauer Farms in LaSalle said various insecticides and other measures did not fight the infestation. “We’re going to take more preventative measures next year,” he said. Psyllids also attack tomato plants, which mean many home gardens have provided a home to the small visitors. The bugs apparently flew right over the San Luis Valley, which produces a large number of

Colorado potatoes. This year, that area is reporting good yields. Source:
<http://www.9news.com/news/article.aspx?storyid=151549&catid=339>

(Illinois) Egg noodles recalled for Salmonella contamination. Real Taste Noodle Manufacture of Chicago, Illinois, announced that the company is recalling its “Egg Noodle” product for possible Salmonella contamination because the egg noodles were made with recalled eggs. The egg noodles subject to recall were distributed to restaurants and grocery wholesalers by pick up or delivery between June 12 and August 25. The noodles were sold in 5-pound bags, with 10 bags per case. The company has not received any reports of illness associated with its products. Source:
<http://www.foodsafetynews.com/2010/09/egg-noodles-recalled-for-salmonella-contamination/>

NOAA reopens more than 3,000 square miles in the Gulf to fishing. NOAA reopened 3,114 square miles of Gulf waters offshore of the western Florida panhandle to commercial and recreational fishing September 3. The reopening was announced after consultation with FDA and under a re-opening protocol agreed to by NOAA, the FDA, and the Gulf states. Trajectory models show the area is at a low risk for future exposure to oil, and fish caught in the area and tested by NOAA experts have shown no signs of contamination. At its closest point, the area to be reopened is about 55 miles northeast of the Deepwater/BP wellhead. The total area is about one percent of federal waters in the Gulf of Mexico. Between August 20 and August 24, NOAA sampled the area for finfish such as tuna, swordfish, and mahi mahi. Sensory analyses of 104 samples and chemical analyses of 101 specimens that were composited into nine samples followed the methodology and procedures in the re-opening protocol, with sensory analysis finding no detectable oil or dispersant odors or flavors, and results of chemical analysis well below the levels of concern. Source:
http://www.noaaneews.noaa.gov/stories2010/20100903_reopening.html

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

Federal Acquisition Regulation needs to toughen safeguards against unauthorized disclosure of sensitive information. Three major federal departments that work closely with sensitive information lack strong safeguards to protect that information, which contractors are accessing while working, according to a report released September 10. The Defense, Homeland Security, and Health and Human Services departments have supplemented the Federal Acquisition Regulation (FAR) with provisions to protect information. However, the additional provisions in DOD’s and HHS’ rules don’t go far enough to protect sensitive information, according to the Government Accountability Office. Also, each department’s supplemental FAR guidance does not specify a contractor’s responsibility to notify officials promptly in case of an unauthorized disclosure or misuse of sensitive information. Looking more broadly, GAO found two important areas that the FAR, the governmentwide rulebook on federal contracting, does not deal with. Regulations don’t deal with the use of nondisclosure agreements as a condition of contractors’ access to information nor do they set a clear process for notifying federal officials quickly about an unauthorized disclosure. In the report, GAO officials recommend that the FAR Council address those issues on a governmentwide basis instead of letting individual agencies write their own provisions. Source:
<http://washingtontechnology.com/articles/2010/09/10/contractors-sensitive-information-disclosure-rules.aspx>

UNCLASSIFIED

(Michigan) Eastern Michigan University investigating computer security breach, employee banking information may be compromised. An Eastern Michigan University computer server was hacked into late September 3, potentially exposing employees' direct deposit banking information, some university passwords and personal identification numbers, according to an e-mail sent to the EMU community September 3. The security breach occurred about 11:30 p.m. September 3, according to the e-mail, and was discovered September 4 by the school's IT staff during routine system monitoring. It happened on a server that controls my.emich passwords and Banner Self-Service PIN codes for students and employees. At this point, there has been no indication of any unusual activity on anyone's accounts, said the EMU vice president of communications. EMU's information technology department is investigating what happened, and the school's Department of Public Safety is opening an investigation as well. An outside data breach consultant is also working with the university. Source: <http://www.annarbor.com/news/eastern-michigan-university-investigating/>

(Florida) Teen girl arrested for St. Augustine High School bomb threat. The 14-year-old suspect behind the August 31 bomb threat at a local high school has been arrested. The suspect was arrested September 1 after the investigation into the threat that led to the evacuation of St. Augustine High School. A caller September 31 told a school receptionist, "There is a bomb in the school," then hung up. Everyone in the school then spent more than two hours in the football stadium, some becoming affected by the heat and requiring medical attention. A student told officials at the school who made the call, but that person denied doing it and was released. Later, another student identified the same person as the caller. When questioned again, the girl admitted to making the call and was arrested. She was released to a parent. The teen faces a charge of making a false bomb threat. Source: <http://www.firstcoastnews.com/news/local/news-article.aspx?storyid=165291&catid=3>

(Texas) 'Suspicious item' leads to lockdown at TSTC. Police locked down four buildings at Texas State Technical College September 3 as they investigated a suspicious object found inside a campus trash container. A campus groundskeeper discovered a "suspicious item" inside the large outdoor trash container at around 2 p.m. outside the school's Rep. Irma Rangel Science and Technology Building, the TSTC Police chief said. Campus police activated the school's emergency notification system and locked down four nearby campus buildings. Harlingen police and a Brownsville police bomb squad rushed to the scene and "deactivated" the device. He would not describe the object and would not give any indication whether it was, in fact, any type of explosive device. The case has been turned over to the federal Bureau of Alcohol, Tobacco, Firearms and Explosives for investigation. The lockdown lasted about a half-hour. Source: <http://www.brownsvilleherald.com/news/tstc-116345-harlingen-item.html>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Anti-US hacker takes credit for 'Here you have' worm. A hacker who claims he was behind a fast-spreading e-mail worm that crippled corporate networks last week said that the worm was designed, in part, as a propaganda tool. The hacker, known as Iraq Resistance, responded to inquiries sent to an e-mail address associated with the "Here you have" worm, which during a brief period early September 9 accounted for about 10 percent of the spam on the Internet. He (or she) revealed no details about his identity, but said, "The creation of this is just a tool to reach my voice to people maybe... or maybe other things." Security experts agree that the worm could have caused more damage. However, it did include some very malicious components, such as password logging

UNCLASSIFIED

software and a backdoor program that could have been used to allow its creator to control infected machines. But because the software was not terribly sophisticated, it was quickly shut down as Web servers that it used to infect machines and issue new commands were taken offline last week.

Source: <http://www.networkworld.com/news/2010/091310-anti-us-hacker-takes-credit-for.html?page=1>

Google's Instant search facility leads to malicious results being offered. Last week saw the release of the latest technology from Google to allow for faster searches. Google called Instant "a new search enhancement that shows results as you type." Effectively it removes the search button with results displayed alongside the text box. The technical director of Panda Security said that there was security concerns when it comes to cyber criminals using Google results as a way to spread malware following the top search terms that people are using in Google searches in order to create fake Web sites. "As users type searches into the real-time engine the opportunity for cyber criminals to infect users through black hat search engine optimisation (SEO) campaigns is increased and Google are potentially putting millions of users at risk. Users should exercise caution when clicking on unknown links and URLs." A detection by Websense found that there were malicious search suggestions appearing as soon as the technology was announced. It said that a search for "anti-virus" produced an "Instant" result for Antivir Solution Pro, a well-known rogueware infection that was amongst the suggested search terms. Source: <http://www.scmagazineuk.com/googles-instant-search-facility-leads-to-malicious-results-being-offered/article/178771/>

Multiple vulnerabilities in Cisco Wireless LAN Controllers. The Cisco WLC family of devices is affected by two denial of service vulnerabilities, three privilege escalation vulnerabilities, and two access control list bypass vulnerabilities. An attacker with the ability to send a malicious IKE packet to an affected Cisco WLC could cause the device to crash and reload. This vulnerability can be exploited from both wired and wireless segments. IKE is enabled by default in the WLC and cannot be disabled. Only traffic destined to the Cisco WLC could trigger this vulnerability. A TCP three-way handshake is needed in order to exploit this vulnerability. Three privilege escalation vulnerabilities exist in the Cisco WLCs that could allow an authenticated attacker with read-only privileges to modify the device configuration. Two vulnerabilities exist in the Cisco WLCs that could allow an unauthenticated attacker to bypass policies that should be enforced by CPU-based ACLs. No other ACL types are affected by these vulnerabilities. Source: <http://www.net-security.org/secworld.php?id=9848>

New fake facebook spam waves sent through cutwail/pushdo botnet. Who said that Cutwail/Pushdo botnet was dead? The recent Cutwail/Pushdo takedown was a great help on stopping this huge botnet in sending spammed messages all over the world. Yesterday, however, a new wave of fake Facebook messages was sent through some Cutwail zombies for about 30 minutes, for a total of approximately 5,000 spammed e-mails. The spammed message informs user that they received a private message and contains a bogus Facebook link which actually points users to a Canadian pharmacy Web site hosted in China. As of this writing, however, the said site is no longer online. This recent Pushdo/Cutwail update shows us that the spammers behind this botnet are on the move, and rebuilding their servers, domains, and the rest of their infrastructure in order to restore their botnet. Source: <http://blog.trendmicro.com/new-fake-facebook-spam-waves-send-through-cutwailpushdo-botnet/>

Cybercriminals hone in on critical systems. In the 2010 threat forecast, “The Future of Threats and Threat Technologies,” Trend Micro researchers mentioned that new attack vectors will arise for virtual/cloud environments. To add to this, critical infrastructures such as a SCADA network will become another serious potential target for cybercriminals. When Trend Micro thinks about SCADA networks or large virtual systems, it is easy to think that these will only be targeted by attackers with espionage in mind whether to take over a factory’s software for hacktivism or to infiltrate a rival’s cloud infrastructure. Unfortunately, a far simpler and more lucrative reason for attacking these targets is to simply blackmail the target organizations and businesses. As bandwidth has increased and the use of content delivery services such as Akamai has become more widespread, network-saturating DDoS attacks have become more difficult, although far from impossible, to carry out. Trend Micro believes that attackers are becoming increasingly innovative in their attacks and that every organization is a potential target. The risks malware pose are now growing from “simple” financial theft to more sophisticated, targeted attacks. Source:

<http://blog.trendmicro.com/cybercriminals-hone-in-on-critical-systems/>

Spammers exploit second Facebook bug in a week. On September 7, Facebook said it has fixed the bug that allowed a spamming worm to automatically post messages to users’ walls earlier this week. The flaw was the second in the past week that let spammers flood the service with messages promoting scams. Recently, Facebook quashed a different bug in its photo upload service that let a spammer post thousands of unwanted wall messages. The newest worm was noticed Monday by researchers at a pair of antivirus vendors, Finland-based F-Secure and U.K.-based Sophos. “A clever spammer has discovered a Facebook vulnerability that allows for auto-replicating links,” said an F-secure security researcher. “Until now, typical Facebook spam has required the use of some social engineering to spread.” Clicking on the link to the bogus application automatically added the app to users’ profiles, then automatically reposted a status message with a new link to friends’ walls, said a prominent researcher at Sophos. Source:

http://www.computerworld.com/s/article/9183879/Spammers_exploit_second_Facebook_bug_in_a_week

Browser security warning lookalike pushes malware. Scareware peddlers have developed a new ruse that relies on mimicking browser warning pages. The malicious code — dubbed Zeven — auto-detects a user’s browser before serving up a warning page that poses as the genuine pages generated by IE, Firefox or Chrome. Prospective marks are warned that their systems are riddled with malware to trick them into running a fake anti-virus software package, called Win7 AV. The warnings are generated from malicious scripts planted on compromised websites. The social engineering scam hinges on the fact a user is more likely to trust a warning and security recommendation ostensibly generated from their browser software than a random “your security is at risk” pop-up. The Win 7 AV scareware package at the center of the scam is served from a site designed to look like the genuine Microsoft Security Essentials website. Source:

http://www.theregister.co.uk/2010/09/06/scareware_fakes_browsers_warnings/

Flash Player as a spy system. If a forged certificate is accepted when accessing the Flash Player’s Settings Manager, which is available exclusively online, attackers can potentially manipulate the player’s website privacy settings. This allows a web page to access a computer’s web cams and microphones and remotely turn the computer into a covert listening device or surveillance camera. At the “Meta Rhein Main Chaos Days 111b,” a Fraunhofer SIT employee presented a scenario in

UNCLASSIFIED

which he used a man-in-the-middle attack (MiTM) to intercept the communication with Adobe's Settings Manager. The Settings Manager itself is a simple Flash applet, and the Adobe pages load it into the browser as an SWF file via HTTPS — a fixed link to it is encoded into the browser. However, the MiTM attack allows attackers to inject a specially crafted applet which manipulates the Flash cookies (Local Shared Objects, LSOs) on the victim's computer. Adobe has been informed about the problem and is considering whether to release a new GUI for the Settings Manager. Source:

<http://www.h-online.com/security/news/item/Flash-Player-as-a-spy-system-1073161.html>

Massive new survey worm spreading on Facebook. A group of developers have found a loophole in Facebook's application Platform which enables them to automatically post messages to a user's wall. This loophole does not require any action by the user, it simply posts to the user's wall the moment they load the application. Right now the messages being spread state "I thought this survey stuff was GARBAGE but i just went on a shopping spree at walmart thanks to FB." This happens to be one of the fastest spreading scams ever seen on Facebook to date, and also one of the largest security glitches in the Facebook Platform. While All Facebook is not aware of any viruses that result from the system, it appears to be the standard offers system which is driving this scam. There appears to be thousands of applications that have been used as part of this scam, which will make it much more time consuming for Facebook to shut down the scammers. Source: <http://www.allfacebook.com/alert-massive-new-survey-scam-spreading-on-facebook-2010-09>

Every week 57,000 fake Web addresses try to infect users. Every week, hackers are creating 57,000 new Web addresses which they position and index on leading search engines in the hope that unwary users will click them by mistake. Those who do, will see their computers infected or any data they enter on these pages fall into the hands of criminals. To do this, they use an average of 375 company brands and names of private institutions from all over the world, all of them instantly recognizable. eBay, Western Union and Visa top the rankings of the most frequently used keywords; followed by Amazon, Bank of America, Paypal and the US revenue service. These are the conclusions of a study carried out by PandaLabs, which has monitored and analyzed the major blackhat SEO attacks of the last three months. Some 65 percent of these fake websites are positioned as belonging to banks. For the most part, they pose as banks in order to steal users' login credentials. Online stores and auction sites are also popular (27 percent), with eBay the most widely used. Other financial institutions (such as investment funds or stockbrokers) and government organizations occupy the following positions, with 2.3 percent and 1.9 percent respectively. The latter is largely accounted for by the US revenue service or other tax collecting agencies. Payment platforms, led by Paypal, and ISPs are in fifth and sixth place, while gaming sites — topped by World of Warcraft — complete the ranking. Source: http://www.net-security.org/malware_news.php?id=1456

NATIONAL MONUMENTS AND ICONS

(Colorado) **Fourmile Fire: 92 structures destroyed, 8 damaged.** Firefighting resources from across the nation continued to arrive in Boulder County, Colorado, as local, state and federal fire crews tried to gain the upper hand on a wildfire that had already burned 100 structures, many of them homes. It was still burning out of control September 8. The Fourmile Canyon Fire was estimated at 7,100 acres with zero percent containment. "Aviation resources today were very helpful in helping firefighters gain ground," said a spokeswoman with the Boulder County Incident Management Team during an evening press conference. "However, the potential for fire spread is still pretty high." Multiple air

UNCLASSIFIED

UNCLASSIFIED

tankers took advantage of calmer winds Tuesday and attacked the fire with a steady barrage of slurry. Officials say more than 90,000 gallons of retardant were dropped on the fire before aircraft had to be grounded due to darkness. Hand crews remained on the ground into the evening. Source:

<http://www.wpix.com/kdvr-boulder-wildfire-txt,0,2164978.story>

(Wyoming) Wildfire prompts evacuation order. A subdivision was evacuated September 7 as a wildfire burned about 37 miles southwest of Laramie, Wyoming, according to a release from Medicine Bow-Routt National Forest officials. The fire, located four miles west of Fox Park, was reported about 2:30 p.m. The fire originated in the Illinois Creek drainage and had burned about 25 acres in beetle-killed lodgepole pine as of early that evening. The Foxborough subdivision was evacuated. There are about 40 homes in the area, many of them second homes. The Albany County Volunteer Fire Department was performing structure protection for the homes. The Medicine Bow-Routt National Forest 20-person fire crew performed the initial attack. One Type I air tanker and two Type III helicopters were expected to arrive late the afternoon of September 7 to begin full suppression. Source: http://billingsgazette.com/news/state-and-regional/wyoming/article_2b6d9e96-baff-11df-8d23-001cc4c03286.html

(Arizona) Arizona signs along I-8 warn of human, drug smuggling violence. Truckers making their way east and west through Arizona may want to avoid areas near Interstate 8. The federal government has posted signs warning of violence and criminals tied to drug and human smuggling. The Bureau of Land Management posted signs this summer warning the public to avoid local routes off of Interstate 8. The highway links Tucson and San Diego, and is a major trucking route that is also used by human and drug smugglers, authorities say. A spokesman with the U.S. Department of the Interior's Bureau of Land Management said his agency put the signs out in June in response to increased danger in a 40-mile area south of I-8 near the Sonoran Desert National Monument. That 487,000-acre desert includes about 200,000 acres south of I-8 that have seen increased drug and human smuggling activity in recent months, the spokesman said September 2. Violence in the area has surged in recent months, though it has not become prevalent on the highway, he said. Instead, authorities are asking travelers to be careful and try to avoid access roads and other areas south of I-8. Source: http://www.landlinemag.com/todays_news/Daily/2010/Sept10/083010/090310-04.htm

POSTAL AND SHIPPING

(Connecticut) Thomaston post office, town hall evacuated. A suspicious letter prompted the evacuation of three buildings in Thomaston, Connecticut, September 7, including the post office and town hall. According to police, the post office received a letter around 9:30 a.m. that claimed there was a bomb in the building. As a precaution the post office, as well as town hall and Center School were evacuated. Authorities did a search of the building and found nothing. The post office is now back open. Police believe they have a suspect and hope to have the case resolved in 24 hours. Source: http://www.wtnh.com/dpp/news/litchfield_cty/thomaston-post-office-evacuated

6 US personnel quarantined over mail scare. The U.S. Embassy in Ankara, Turkey, says six U.S. army post office personnel have been quarantined after handling a package containing a powdery substance at Istanbul's main airport. A U.S. Embassy spokeswoman said September 3 the six were quarantined pending laboratory results to determine whether the powder is a dangerous substance, such as anthrax. The results were expected September 11. The embassy spokeswoman said a health

UNCLASSIFIED

UNCLASSIFIED

team has decontaminated the area and the six are being administered antibiotics as a precaution at a hospital in Istanbul. The personnel deliver U.S. diplomatic mail in Turkey. Source:

<http://www.google.com/hostednews/ap/article/ALeqM5i6Bh-b-fx2pu42ihmUv9g6UxuerwD9I0BUVG0>

PUBLIC HEALTH

(Illinois) Pertussis reported in Illinois. Over 445 cases of pertussis have been reported in Illinois to date, with 65 percent of those reported since May of this year. Of the cases reported since May, 45 percent have occurred among school-aged children; over 30 percent have occurred in children under five years of age. Source: <http://www.reviewatlas.com/news/x907383692/Pertussis-reported-in-Illinois>

New 'superbug' may endanger global health. Japanese experts say they fear an enzyme that turns bacteria into superbugs resistant to antibiotics may be able to similarly affect poisonous bacteria. A case of NDM-1, resistant to virtually all antibiotics, was found in its first Japanese victim Monday, Tokyo's Yomiuri Shimbun reported. The feverish patient, a man in his 50s, was found to have E. coli affected by the NDM-1 enzyme. He was discharged after being treated, Yomiuri Shimbun reported. Medical experts fear poisonous bacteria such as salmonella and dysentery bacillus may become superbugs resistant to antibiotics, the newspaper said. Since the superbug was discovered in India, it has spread to Britain and the United States through patients who had surgeries in India. The first death directly attributed to NDM-1 was reported last month in Belgium, the newspaper said. Source: http://www.upi.com/Top_News/International/2010/09/07/New-superbug-may-endanger-global-health/UPI-50651283877124/

(California) Vaccinated people getting whooping cough in SD. A KPBS investigation has raised questions about how effective the whooping cough vaccine is in preventing people from getting sick. Nearly two out of three people diagnosed with whooping cough in San Diego County this year, were fully immunized. California is in the midst of the worst whooping cough epidemic in 50 years. Thirty six hundred people in the state have been diagnosed with the disease. Eight babies have died since January. KPBS examined data from San Diego County's Health and Human Services Agency. Of the 332 confirmed cases of whooping cough in the county so far this year, 197 of the people who got sick were up to date with their immunizations. That is nearly 2 out of 3 cases. Source: <http://www.kpbs.org/news/2010/sep/07/vaccinated-people-getting-whooping-cough-sd/>

(California) Planned Parenthood clinic in California damaged. Federal and local authorities are investigating a fiery after-hours attack on a Planned Parenthood clinic in California. Madera police say someone threw a makeshift explosive through the clinic's window early the morning of September 2, breaking the glass and burning blinds. Police say this is the first violent crime they have seen against the clinic, which has been open for 20 years. A clinic spokeswoman says the office will remain closed through the Labor Day weekend and reopen September 7. Source: <http://www.google.com/hostednews/ap/article/ALeqM5ghCU3w53giat9KYAuazOFcJvuNeAD9I0M2E00>

(Maryland) Swine flu less severe, but still around. Earlier this month, the World Health Organization (WHO) declared an end to the global pandemic of the virus, which officially is called H1N1. "The new

UNCLASSIFIED

UNCLASSIFIED

H1N1 virus has largely run its course,” said a WHO’s director-general, But, she warned, that doesn’t mean H1N1 is gone for good. It turns out that H1N1 may be turning into yet another strain of flu that circulates during flu season. “It’s kind of run its course. Since we have some immunity in the population, it turns into any other seasonal influenza,” said an acting deputy county health officer in Maryland. Source: <http://www.hometownannapolis.com/news/nbh/2010/09/07-09/Swine-flu-less-severe-but-still-around.html>

(Georgia) Army: Ex-soldier takes 3 hospital workers hostage. A former Army soldier seeking help for mental problems at a Georgia military hospital took three workers hostage at gunpoint September 6 before authorities persuaded the gunman to surrender peacefully. A Fort Stewart spokesman said no one was hurt and no shots were fired in a short standoff at Winn Army Community Hospital on Fort Stewart, about 40 miles southwest of Savannah. Military officials said the hostages were able to calm the gunman and keep him away from patients until he surrendered. The gunman was arrested by military police. The gunman walked into the hospital’s emergency room at about 4 a.m. carrying four guns — two handguns, a semiautomatic rifle, and a semiautomatic version of a submachine gun, a senior Fort Stewart commander said. He had seen nothing to indicate the former soldier had previously sought treatment at the Fort Stewart hospital. Source: http://www.google.com/hostednews/ap/article/ALeqM5j6HgufyKkYWaB_j7NclbAlhjkWbwD9l2KSMO1

TRANSPORTATION

Panel: Commercial flights remain top terror targets. Commercial aviation remains the top target for terrorists who are likely to try again to use an easily hidden bomb to blow up an airplane, according to a report released September 10 by former leaders of the 9/11 Commission. The report cites the bombmaker who put together the powdered-explosive device that a Nigerian man hid in his underwear and tried to detonate on a Northwest Airlines flight over Detroit on Christmas Day in 2009. The bombing attempt failed, but the bombmaker, whom the report does not name, “is still at large” and “is likely to try to bring down another commercial jet with a concealed bomb that is not detectable by metal detectors,” the report says. In addition, al-Qaeda could try to blow up a jet with a surface-to-air missile, according to the report, which was released by the former 9/11 Commission chairmen. The two men now head the National Security Preparedness Group of the Bipartisan Policy Center, a Washington, D.C. organization. The 37-page report, Assessing the Terrorist Threat, says that other top targets are distinctive brand names, particularly American hotel chains, as well as Israeli and Jewish people and buildings. Source: http://www.usatoday.com/news/nation/2010-09-10-flights-terror-targets_N.htm

(Michigan) FBI investigates who aimed lasers at pilots. The FBI is trying to determine who aimed laser lights at pilots flying out of Selfridge Air National Guard Base in Michigan twice in the last two weeks. A helicopter pilot flying over Madison Heights two weeks ago called police there when a beam came into the cockpit, a U.S. Customs and Border Protection spokesman said September 9. Investigators questioned a man who lives at the Madison Heights home where the light originated, but no one has been charged. In a separate incident, a pilot on final approach to Selfridge late last week reported seeing a laser light aimed into the cockpit. Source: <http://www.freep.com/article/20100910/NEWS03/9100314/1322/Local-news-in-brief--FBI-investigates-who-aimed-lasers-at-pilots>

UNCLASSIFIED

UNCLASSIFIED

(Massachusetts) Suicide prompts cyanide search at train station. A woman's suicide led police to search for cyanide at a Massachusetts train station. Police say a former Northeastern University lab technician took her own life by ingesting crystallized cyanide. According to investigators, the woman took a train into Boston Saturday and entered a Northeastern lab. Authorities say she left her car at the Westwood commuter rail station. The state police bomb squad and a Hazmat team searched the car. No dangerous materials were located and there reportedly was no threat to commuters. Police say it is still not clear where she obtained the cyanide. Source:

<http://www1.whdh.com/news/articles/local/12002204137364/commuter-rail-searched-for-cyanide/>

(Alabama) Greyhound bus cleared after bomb scare. Though the man behind a bomb threat September 8 was in custody more than 200 miles away, the scare he created stayed aboard a bus and made its way to Tuscaloosa, Alabama. The Tuscaloosa Police Department's bomb squad along with FBI agents and members of the bureau's Joint Terrorist Task Force responded to a BP gas station near Duncanville on Highway 82 to perform a bomb search on a Greyhound bus. The officers and agents did not find a bomb and sent the bus on its way. A spokesman for the FBI's Birmingham division said a Nigerian man boarded a bus in an unknown Mississippi town. "Once he was on board, he claimed he had a bomb and was going to blow up the bus," the spokesman said. The man was arrested and charged with making terrorist threats. However, because the bus driver told officers the man did not bring any luggage onto the bus, the bus was not searched for a bomb after he was taken into custody. "But later on, the Nigerian man did tell police that he did have luggage on the bus," the FBI spokesman said. "By that time, the bus was near Tuscaloosa and it was stopped at the (gas station) where it was searched." Source:

<http://www.tuscaloosaneews.com/article/20100908/NEWS/100909655/1007?tc=ar>

Security program trains truckers. After the first two years of a three-year program, 18,100 truckers have completed training in a federally funded trucking security program known as First Observer. In August 2008, the U.S. Department of Homeland Security awarded a \$15.5 million grant to administer an anti-terrorism and security awareness program for highway professionals. The program's First Observer component is to recruit and train industry volunteers to report suspicious activities that might be criminal or linked to terrorism to authorities. First Observer's training modules are also targeted to workers in law enforcement, cargo and supply chain, infrastructure, hazmat, highway, ports and truck rental and leasing. It has 57,000 members and 90 industry affiliates and supporters, according to FEMA. The latter includes motor coach associations, emergency preparedness personnel, truck driver training organizations, parking associations and airport ground personnel. Source: <http://www.etrucker.com/apps/news/article.asp?id=85765>

WATER AND DAMS

(Michigan) Police investigating breach at Kalamazoo's water supply. Tests of water samples from two water-storage facilities in Kalamazoo, Michigan that were recently breached show that the city's water supply has not been contaminated, police and city officials said September 9. Officials from the department of public services collected bacteriological and chemical samples from storage facilities on Beech, Blakeslee, and North Dartmouth streets after Public Safety officers were called September 7 to the Blakeslee and Dartmouth sites and found that fencing at both locations had been cut. Officials said they still plan to drain and inspect a storage tank at the Blakeslee facility early

UNCLASSIFIED

UNCLASSIFIED

September 10 that was breached during the incidents. The tank will be cleaned and disinfected and water samples will be taken from the tank for further testing before it is put back into service late next week. Meanwhile, police are increasing patrols near the city's water storage facilities, the public safety chief said. Source:

http://www.mlive.com/news/kalamazoo/index.ssf/2010/09/update_officials_say_further_t.html

(Oklahoma) Contaminated water widespread in state. Nearly 140 public water supplies in Oklahoma are operating in consistent violation of state and federal drinking water codes, pumping water that contains chemicals linked to cancer, infant illness, and damage to the liver and nervous system. Nine public water sites serving about 16,000 customers in central Oklahoma have orders to resolve environmental compliance issues, records from the state Department of Environmental Quality show. The department regulates 1,582 public water systems. "The public has a right to know about the quality of their drinking water," a department spokeswoman said. "Some of these things might not hurt them for several decades, but they have the right to know." Source:

http://www.tulsaworld.com/news/article.aspx?subjectid=11&articleid=20100907_12_A4_CUTLIN249280

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7):** 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: 701-328-8175

State Radio: 800-472-2121 **Bureau of Criminal Investigation:** 701-328-5500 **Highway Patrol:** 701-328-2455

US Attorney's Office Intel Analyst: 701-297-7400 **Bismarck FBI:** 701-223-4875 **Fargo FBI:** 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED